

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

IN THE MATTER OF THE ISSUANCE
OF A CRIMINAL COMPLAINT RE:

SHANNON ROBBINS

Case No. 2:24-mj-29

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Rachel Foss, being duly sworn, hereby depose and state:

I. INTRODUCTION

1. I am a Task Force Officer (TFO) with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been a TFO since September 2019 with HSI. Additionally, I have been employed by the City of Virginia Beach, Virginia, as a police officer since August 2007 and as a police detective since March 2012. In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and child pornography. Since joining the Virginia Beach Police Department (VBPD) and becoming a TFO with HSI, I have received specialized training in child exploitation investigations, identifying and seizing electronic evidence, and social website investigations. I have also received specialized training in undercover chat investigations and operations. Additionally, I have received instruction and practical application in peer-to-peer investigations and forensic field triage. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is submitted in support of a criminal complaint and arrest warrant charging defendant Shannon ROBBINS with receipt and distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2); sales of child pornography, in violation of 18 U.S.C. § 2252(a)(3); possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B); coercion and enticement of a minor, in violation of 18 U.S.C. § 2422(b); and transfer of obscene material to a minor, in violation of 18 U.S.C. § 1470.

4. This affidavit is based on my personal observations during this investigation, information conveyed to me by other law enforcement officials, my review of records, documents and other physical evidence obtained during this investigation, and interviews of witnesses. This affidavit contains information necessary to support a finding of probable cause, but does not include each and every fact observed by me or known by the government.

II. SUBJECT OF INVESTIGATION

5. Shannon ROBBINS is a United States citizen who was last known to reside in Virginia Beach, Virginia, in the Eastern District of Virginia. He is charged in the Virginia Beach Juvenile and Domestic Relations Court with 10 counts of possession, reproduction, distribution, solicitation, or facilitation of child pornography, in violation of VA. CODE ANN. § 18.2-374.1:1, arising out of this investigation. He is being held without bond in that case.

III. LEGAL AUTHORITY

6. Under 18 U.S.C. § 2252(a)(2), it is unlawful, in relevant part, knowingly to receive or distribute any visual depiction using any means or facility of interstate or foreign

commerce or that has been mailed, or that has been shipped or transported in or affecting interstate or foreign commerce, by any means including by computer, if —

- the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
- such visual depiction is of such conduct.

7. Under 18 U.S.C. § 2252(a)(3), it is unlawful, in relevant part, knowingly to sell any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or has been shipped or transported in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported using any means or facility of interstate or foreign commerce, including by computer, if —

- the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
- such visual depiction is of such conduct.

8. Under 18 U.S.C. § 2252(a)(4)(B), it is unlawful, in relevant part, knowingly to possess one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if —

- the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
- such visual depiction is of such conduct.

9. Under 18 U.S.C. § 2422(b), it is unlawful, in relevant part, using any facility or means of interstate or foreign commerce, knowingly to persuade, induce, entice, or coerce any

individual less than 18 years of age to engage in any sexual activity for which any person can be charged with a criminal offense.

10. Under 18 U.S.C. § 1470, it is unlawful, in relevant part, using any facility or means of interstate or foreign commerce, knowingly to transfer obscene matter to another individual less than 16 years of age, knowing that such other individual is less than 16 years of age.

IV. DEFINITIONS

11. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involves the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. In this affidavit, I will also refer to “child pornography” as “child sexual abuse material” (“CSAM”).

12. The term “computer,” as used in this affidavit, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” As used in this affidavit, a computer includes wireless telephones and other mobile computing devices like tablets.

13. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A

password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

14. “Contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

15. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (“ISP”) that connects to the Internet. Internet service providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. The ISP assigns each user an Internet Protocol (“IP”) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s

customers or subscribers. Thus, by ascertaining the IP address relating to a specific message sent or action taken over the Internet, it is possible to determine the ISP and even the individual computer responsible.

16. The terms “minor” and “sexually explicit conduct” are defined in 18 U.S.C. §§ 2256(1) and (2), respectively. A “minor” is defined as “any person under the age of 18 years.” The term “sexually explicit conduct” means actual or simulated —

- sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- bestiality;
- masturbation;
- sadistic or masochistic abuse; or
- lascivious exhibition of the anus, genitals, or pubic area of any person.

17. The terms “records,” “documents,” and “materials” include all information recorded in any form, including the originals and all nonidentical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following: graphic records or representations, photographs, pictures, images, and aural records or representations.

18. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

V. PROBABLE CAUSE

A. Inception of the investigation

19. In August 2023, Matt Hedden, a detective in the Department of Criminal Investigations in the Kentucky Office of the Attorney General, contacted me regarding an investigation he was working involving the online distribution of CSAM. Hedden learned that a subject, Witness 1, was paying a minor child, Minor Victim 1, to take sexually explicit pictures of Minor Victim 1 and send them to Witness 1. Witness 1 paid Minor Victim 1 through a payment platform called Cash App, which is accessible by most cell phones. Witness 1 was interviewed by Hedden and confessed to the crimes. Hedden's investigation also revealed that Witness 1 was purchasing CSAM from an unidentified subject with whom Witness 1 communicated on Telegram between March and August 2022. Telegram is an encrypted messaging and file-exchange application commonly used on mobile phones.

20. Witness 1 consented to Hedden's review of Witness 1's cell phone. On it, Hedden located several items of relevance to his investigation, including multiple files of CSAM, financial transactions from Cash App, and a Telegram conversation with an unknown subject in which Witness 1 purchased CSAM files. Among those files exchanged through Telegram were at least two sexually explicit video files of Minor Victim 1. Hedden requested and received records from Block, Inc., which owns Cash App.

B. An unidentified subject sells Witness 1 CSAM using Telegram and Cash App

21. Witness 1's Cash App records showed that, on August 20, 2022, Witness 1 received, via Cash App, a request for \$50 from another Cash App user who employed the display name **Cash App User 1**. (Usernames and display names referred to in this affidavit are known to law enforcement but will be replaced with pseudonyms here because their public availability may compromise an ongoing investigation.) Based on my training and experience, I believe that the true purpose of this "request" was not to solicit money, but to send a text-based message to

Witness 1. At the option of the user sending or requesting funds using Cash App, a short message may be conveyed with the payment or request. The message accompanying **Cash App User 1**'s request to Witness 1 was "message me on tele ASAP." Based on my training and experience, I believe that "tele" was an abbreviation of Telegram and that **Cash App User 1** was directing Witness 1 to initiate contact with **Cash App User 1** via Telegram.

22. After about 10 minutes elapsed and **Cash App User 1** received no response from Witness 1, **Cash App User 1** sent another Cash App request to Witness 1. The request was for \$1 and carried the message "message on tele ASAP it's a BIG deal." Witness 1 then sent **Cash App User 1** a false \$1 payment request that carried this message: "what is your telegram again? I made a new acc[ount]." **Cash App User 1** responded — through another false \$1 payment request on Cash App — with the Telegram username **Telegram User 1**.

23. Data extracted by consent from Witness 1's phone showed that, about one minute later, Witness 1 began to communicate with **Telegram User 1** on Telegram, beginning with Witness 1 messaging **Telegram User 1**, "Hey I got your cashapp message." The following exchange then ensued:

Telegram User 1: Anyway I got some good stuff over the last 2 weeks

Witness 1: Oooo really?

[At this point, **Telegram User 1** sent three non-CSAM photographs of juvenile boys approximately 12 to 13 years of age.]

* * *

Telegram User 1: Whenever [sic] u get some money let me know

Witness 1: Well how much would you charge?

Telegram User 1: Depends on what u want like last time

Telegram User 1: U just tell me what u have to spend

Witness 1: I'm kinda in the mood for pictures, like the ones you sent

Telegram User 1: Wym [What do you mean?]

Telegram User 1: Clothed pics[?]

Telegram User 1: Or nudes[?]

Witness 1: Both

Telegram User 1: Ok

Telegram User 1: Make an offer

Witness 1: How does \$100 sound[?]

Telegram User 1: Ok that works

24. **Telegram User 1** gauged the age of Witness 1's interest by asking whether Witness 1 preferred "[s]ome hair [or] no hair." Based on my training and experience, I believe **Telegram User 1** was referring to pubic hair on the boys depicted in the CSAM files that Witness 1 was to purchase from **Telegram User 1**.

25. Witness 1 then received a Cash App request for \$100 from **Cash App User 1**. The message attached to the payment request was "training." Although the message was false, the payment request was not, and Witness 1 fulfilled the request by sending **Cash App User 1** \$100.

26. **Telegram User 1** then sent Witness 1 several images and videos of CSAM via Telegram. The approximate age range of the depicted victims, all boys, is 12 to 14 years of age. The CSAM depicts masturbation and lascivious exhibition of the victims' genitals and anuses.

27. In the Telegram conversation, Witness 1 identified one boy of whom he requested more CSAM. **Telegram User 1** told Witness 1 that his collection of this boy was "290 pieces" and told Witness 1 to make **Telegram User 1** an offer. When Witness 1 expressed doubt that he

could afford what the asking price would be, **Telegram User 1** offered to sell the lot for \$100. Witness 1 agreed, adding that he wanted to see other boys.

28. Witness 1 then sent **Cash App User 1** \$100 through Cash App.

29. In response to Witness 1's request to see what other CSAM could be had, **Telegram User 1** sent Witness 1 a video. This video was a screen recording, which is a video file that shows the contents of a phone screen exactly as the recording user sees it. In the recording, the user scrolls through a photo application that I now believe to have been Private Photo Vault. As the screen recording progresses, a Telegram message from Witness 1 appears on the top of the screen, which justifies my conclusion that this screen recording was created during **Telegram User 1's** Telegram conversation with Witness 1, and not at some other time, by the same person who controlled the **Telegram User 1** Telegram account. The photo application showed several boys of the same approximate age range as the CSAM that Witness 1 earlier received from **Telegram User 1**. The name of the folder of images in which the user was demonstrating their collection was "2021/2022."

30. Around this time, Witness 1 asked **Telegram User 1** whether they had received Witness 1's second \$100 payment. **Telegram User 1** responded affirmatively and sent to Witness 1 14 images and six videos depicting a boy of 12 to 13 years of age engaging in masturbation and lascivious exhibition of his genitals.

31. The following day, August 21, 2022, in a similar exchange, Witness 1 purchased additional CSAM from **Telegram User 1**, sending \$75 through Cash App to **Cash App User 1**.

32. On August 26, 2022, Witness 1 purchased additional CSAM from **Telegram User 1** by sending \$100 through Cash App to **Cash App User 1**.

C. Subpoenas to Verizon and Block, Inc.

33. Hedden determined that the phone number (757) 880-0522 was associated with Telegram user **Telegram User 1**. Open-source investigation revealed that this number was serviced by Verizon. Further investigation revealed that the owner of the Verizon account was Shannon ROBBINS, date of birth XX/XX/1973, who provided an address in Virginia Beach, Virginia, which is within the Eastern District of Virginia.

34. Hedden also determined that the Cash App account to which Witness 1 directed his payments was associated with the unique identifier token **Cash App Token 1**.

35. After he served a subpoena on Block, Inc., which owns Cash App, for records associated with the token **Cash App Token 1**, Hedden received Block's responsive records and reviewed them. One of the active email addresses listed was **Email Address 1**.

36. There were 372 transactions between July 28, 2022 and July 19, 2023. As expected from his interactions with the cooperative Witness 1, Hedden observed among the **Cash App User 1** account's records the transactions between **Cash App User 1** and Witness 1 described above.

37. Hedden observed 22 transactions between **Cash App User 1** and Minor Victim 1's Cash App account. Over 22 transactions, **Cash App User 1** sent Minor Victim 1 approximately \$330. Witness 1 explained that both he and **Telegram User 1** paid Minor Victim 1 for self-produced CSAM. Accordingly, I believe that these 22 payments to Minor Victim 1 were for the purchase of Minor Victim 1's self-produced CSAM.

D. Evidence that the Cash App User 1 and Cash App User 2 accounts were controlled by Shannon Robbins

38. Hedden noticed several transactions between the **Cash App User 1** Cash App account and another account that used the display name **Cash App User 2**. He observed that

Cash App User 2 appeared to be the primary funding source for the **Cash App User 1** account, having sent **Cash App User 1** approximately \$3,219 over 59 transactions.

39. Cash App logs the IP address of its users each time a transaction is attempted and includes this data in its subpoena returns. Hedden determined that one IP address, 108.39.96.131, appeared with the greatest frequency in the **Cash App User 1** account.

40. Cash App records for the **Cash App User 2** account show that **Cash App User 2** used the same Verizon IP address on numerous occasions within the same period. This suggests that **Cash App User 1** and **Cash App User 2** logged in to the two Cash App accounts from the same location.

41. After determining that the 108.39.96.131 IP address belonged to Verizon, I served a subpoena on Verizon for the subscriber information associated with that IP address. Responsive records revealed that the IP address was assigned to Shannon ROBBINS in Virginia Beach, Virginia, which is within the Eastern District of Virginia, beginning on November 7, 2022, and remained assigned to ROBBINS in August 2023 when Verizon received my subpoena. The daytime telephone number associated with ROBBINS's Verizon account was (757) 880-0522, which was also associated with the **Telegram User 1** Telegram account. The listed email address was **srobbinsx10@gmail.com**.

42. Cash App records provide the name of the device, usually a cell phone, that is used to attempt a transaction on behalf of the subject account. A device's name may be changed by its owner. In the case of the **Cash App User 1** account, the name of the device used to attempt transactions from July 19, 2022 through September 16, 2022 was **Shannon**. Beginning on September 17, 2022, the primary device name seen on the **Cash App User 1** account is **iPhone**. This is likely because the user activated a new phone, as evidenced by the

contemporaneous alteration of the device model from D63AP, shorthand for the iPhone 13 Pro, to D73AP, which designates the iPhone 14 Pro. When this phone change occurred, the version of the phone's operating system, iOS, changed from 15.6.1 to 16.0.1.

43. Examination of Cash App records for the **Cash App User 2** account showed that the primary device used to connect to this account underwent identical changes at the same time. That is, the phone used to connect to the **Cash App User 2** account from July 19, 2022 through September 16, 2022 was an iPhone 13 Pro named **Shannon** that ran iOS 15.6.1; and on September 17, 2022 became an iPhone 14 Pro named **iPhone** that ran iOS 16.0.1.

44. On October 3, 2022, using Cash App, **Cash App User 2** sent **Cash App User 1** \$30 using a Bank of America card ending in 8805. Legal process to Bank of America revealed that the owner of the 8805 account was Shannon ROBBINS. At the time of this transaction, Cash App accounts **Cash App User 2** and **Cash App User 1** used the same IP address, 71.120.148.214. I learned from Verizon records that this IP address was assigned to Shannon ROBBINS during the time of this transaction. Additionally, as suggested above, **Cash App User 2** and **Cash App User 1** used the same model device — an iPhone 14 Pro — and the same version of iOS — 16.0.2 — at the time of this exchange. Based on this evidence and my training and experience, I believe that this \$30 transaction consisted of ROBBINS funding his own second Cash App account (**Cash App User 1**), which he used in part to purchase and sell CSAM.

45. According to Bank of America records, the access IDs associated with ROBBINS's credit-card account ending in 8805 combined to log in with the IP address 108.39.96.131, which was frequently used by both the **Cash App User 1** and **Cash App User 2** Cash App accounts, over 2,000 times in approximately 12 months.

46. Unlike the **Cash App User 1** account, the **Cash App User 2** Cash App account contained identity information purported, by Block, to have been verified. The owner of the **Cash App User 2** account was listed as Shannon ROBBINS, date of birth XX/XX/1973. The same address in Virginia Beach, Virginia, within the Eastern District of Virginia, was provided that was found in Verizon and Bank of America records. The active email address is **srobbinsx10@gmail.com**, which was likewise listed in ROBBINS's Verizon and Bank of America records.

47. As detailed above, Witness 1 paid **Cash App User 1** for CSAM delivered through Telegram by **Telegram User 1**. But before that, Witness 1 paid **Cash App User 2** — the Cash App account that was explicitly associated with ROBBINS — directly. From July 22, 2022 to August 6, 2022, Witness 1 sent \$200 over four transactions to **Cash App User 2**. Telegram messages pertaining to these transactions are not available. As Witness 1 explained to **Cash App User 1**, Witness 1 created a new Telegram account, which would explain the unavailability of these earlier messages.

E. Forensic review of Robbins's cell phone

48. On October 24, 2023, a magistrate with the City of Virginia Beach district court authorized a search of ROBBINS's residence and the seizure and forensic review of electronic devices. The search and seizure warrant was executed on October 25, 2023. Among the items collected was ROBBINS's iPhone, which was placed into airplane mode to protect the integrity of the data thereon.

49. ROBBINS's phone contained a text-message conversation between the user of the phone, whom I believe to have been ROBBINS, and Minor Victim 2, who told ROBBINS that his age was 13. In the conversation, ROBBINS assumes the identity of another 13-year-old male

who ROBBINS represents to be bisexual. ROBBINS sent to Minor Victim 2 at least three CSAM images of a juvenile male, and one CSAM video of a juvenile male masturbating.

50. From my training and experience, and the context of the text-message conversation, it appears to me that ROBBINS's objective was for the 13-year-old Minor Victim 2 to self-produce CSAM and send it to ROBBINS. For example, ROBBINS sent the following message to Minor Victim 2: "Show me u in boxers only or ur ass or dick so I can jerk." When the victim persistently refused to provide explicit images of himself, ROBBINS asked, "When will u get freaky with me[?]" Minor Victim 2 has since been identified.

51. ROBBINS's phone contained evidence of three accounts and passwords for which **Email Address 1** was the username. This same email address was associated with the Cash App records for **Cash App User 1**, which sold CSAM to Witness 1. In one instance, the decrypted password for the account was **Manager**05\$**. This password was significant to me because I learned that ROBBINS managed fast-food restaurants and **05 was his house number. (The full four-digit number is known to law enforcement.)

52. When **Cash App User 1** used Cash App to contact Witness 1 on August 20, 2022, **Cash App User 1** said that their Telegram username was **Telegram User 1**.

53. On September 19, 2022, **Cash App User 1** provided a new Telegram username, **Telegram User 2**, to another Cash App user.

54. When ROBBINS's phone was seized, the Telegram application was installed on ROBBINS's phone and logged into Telegram as user **Telegram User 2**.

55. I observed that ROBBINS's phone contained a large volume of CSAM image and video files. The majority of the CSAM files were maintained in an application called Private Photo Vault. (Despite the name of the application, Private Photo Vault also facilitated the

storage and viewing of video files.) The images and videos kept in this application are not accessible unless the owner of the phone provides the phone's passcode or satisfies a biometric challenge such as Apple's Face ID. My training and experience lead me to believe that ROBBINS used Private Photo Vault to hide his collection of CSAM.

56. The CSAM in the Private Photo Vault application was largely organized by apparent names of the depicted victims: in some instances both their first and last names. Using these names and other information, my investigation has identified several of the victims whose CSAM appears on ROBBINS's phone. Some of the victims were social acquaintances of ROBBINS and his family and frequented his house in Virginia Beach, Virginia.

57. I also located artifacts of CSAM in other areas on ROBBINS's phone. For example, I located the following video files:

- 11 Year Old [*first name withheld*] Jerks 5.avi
- 10 Year Old Blond Cutie Jerks And Toothbrushes Ass.avi
- 8 Year Old Mushroom Head Cutie Finally Jerks Off.avi

I personally reviewed these video files and determined that they constitute child pornography as defined by 18 U.S.C. § 2256(8).

F. CyberTipline reports connected to Robbins

58. On September 8, 2022, the National Center for Missing and Exploited Children ("NCMEC") received CyberTipline Report #133945022. The report was made by Snap, Inc., which owns the Snapchat messaging application, after Snap determined that a Snapchat user had saved, shared, or uploaded four files of suspected child pornography. NCMEC classified the material as apparent child pornography. Snap reported that the IP address used to connect to

Snapchat was 71.120.148.214. Cross-referencing its records, NCMEC determined that the same IP address was associated with two other CyberTipline reports.

59. On September 19, 2022, NCMEC received CyberTipline Report #135190929. This report, too, was generated by Snap in response to activity on its Snapchat application. The offending IP address, 71.120.148.214, was identical to the September 8, 2022 report. In this second report, Snap identified 17 files of suspected child pornography on Snapchat. Using NCMEC's categorization system, Snap classified 11 files as prepubescent minors engaging in sex acts, four files as pubescent minors engaging in sex acts, and two files as pubescent minors engaging in lascivious exhibition.

60. NCMEC defines a "sex act" as any imagery depicting sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction of the above that lacks serious literary, artistic, political, or scientific value. "Lascivious exhibition" is defined as any imagery depicting the lascivious exhibition of the anus, genitals, or pubic area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child's anus, genitals, or pubic area and where the depiction is intended or designed to elicit a sexual response in the viewer.

61. From September 8, 2022 to September 19, 2022, the period from the first CyberTipline report to the second, the **Cash App User 1** account used the same IP address 10 times. This includes transactions sent to Witness 1 directing him to reestablish contact through Telegram. (Unbeknownst to ROBBINS, Witness 1 was arrested on September 2, 2022.) According to Verizon records, the IP address 71.120.148.214 was assigned to the ROBBINS

residence in Virginia Beach, Virginia, within the Eastern District of Virginia, continuously from April 2022 to November 2022, with the exception of an anomalous three-second period on September 13, 2022, from 6:49:35 a.m. to 6:49:38 a.m.

G. Robbins's use of other social media

62. My investigation has shown that ROBBINS regularly created numerous accounts on Instagram, Snapchat, and TikTok as part of his attempts both to evade detection and to deceive his child victims. Further, during Hedden's investigation, Witness 1 admitted that, in addition to communication via Telegram, he used Snapchat to communicate with the person who identified themselves on Telegram as **Telegram User 1**.

63. Because I found on ROBBINS's phone several screenshots of juvenile boys that originated from Snapchat, I believe that ROBBINS used Snapchat as a method for meeting, communicating with, and manipulating juvenile boys.

64. Data from ROBBINS's phone and Cash App records from the **Cash App User 1** account show that ROBBINS used Snapchat to communicate with Minor Victim 1. The content of these messages is not available, but the date and time of each Snapchat message is visible and they are interspersed with **Cash App User 1**'s Cash App payments to Minor Victim 1. Accordingly, it is my opinion that ROBBINS sent Snapchat messages to Minor Victim 1 directing Minor Victim 1 to self-produce CSAM, sent money to Minor Victim 1 using Cash App, received CSAM from Minor Victim 1 on Snapchat, and saved the CSAM to ROBBINS's phone in the Private Photo Vault application where I ultimately found it.

65. Based on the appearance of similarly structured Cash App payments with similar sham messages attached to them, Hedden opined based on his training and experience, and I agree independently based on my own training and experience, that ROBBINS was engaging in

similar behavior with other minor children using a combination of Snapchat and Cash App; that is, that ROBBINS was paying minor children for self-produced CSAM.

66. On October 3, 2023, in a Telegram conversation with a user with whom ROBBINS (as **Telegram User 2**) exchanged CSAM, ROBBINS explained to the user that ROBBINS needed an audio recording of a girl saying “Hi Jake.” Based on the context of this conversation, and my training and experience, I believe that, in a separate conversation, ROBBINS was communicating with a juvenile male named Jake while impersonating a like-aged female. This is known as “baiting,” and I found ample evidence that ROBBINS engaged in baiting juvenile males in attempts to have the juveniles self-produce CSAM and send it to ROBBINS under the false impression that they were sending depictions of themselves to other juveniles.

67. In the Private Photo Vault application on ROBBINS’s phone, I located a folder with the name of Minor Victim 3, who was personally acquainted with ROBBINS. Inside the folder I located at least two images depicting Minor Victim 3 that constitute child pornography as defined by 18 U.S.C. § 2256(8). In the first image, Minor Victim 3’s penis is depicted and appears to be the focus of the image. In the second image, Minor Victim 3 wears underwear but has a visible erection. Based on my training and experience, these images lasciviously exhibit Minor Victim 3’s genitals. In an interview with me, Minor Victim 3 stated that he was contacted on Snapchat by a user posing as a girl and asked to send self-produced CSAM to the user, which he did. I reviewed a screenshot of the Snapchat profile of this user and noted that the username was **Snapchat User 1**. This was significant to me because, as I described above, ROBBINS’s phone contained a Telegram conversation in which ROBBINS told a fellow CSAM trader that ROBBINS’s Snapchat username was **Snapchat User 1**.

68. I sent an administrative subpoena to Snap, Inc. for subscriber information relating to the **Snapchat User 1** account. According to the records I received in response, the IP address used to create this account was 108.39.96.131, which is connected to ROBBINS's residence, as I described above.

69. Following seizure of ROBBINS's cell phone, I physically reviewed the contents of the phone on or about October 28, 2023. I observed that the phone was logged in to Snapchat with a username that was a permutation of a common pseudonym that ROBBINS used to disguise his identity, to deceive minor victims into self-producing CSAM, and/or to purchase and sell CSAM, in violation of one or more of the Target Offenses. Records from Snap, Inc. show that previous display names that were used by this account included the terms "leaked," "exposed," and "nudes," accompanied by male first names. Based on my training and experience, and the context of my investigation, I believe that these display names referred to the distribution of CSAM.

70. On January 11, 2024, I interviewed Minor Victim 4, who was personally acquainted with ROBBINS. I located several CSAM images depicting Minor Victim 4 on ROBBINS's phone. Minor Victim 4 stated that, in or about June 2023, they sent CSAM of themselves to one Instagram account, the owner of which account represented to Minor Victim 4 that they were a young female, and to no other person or account. Based on this information and my training and experience, I believe that ROBBINS obtained CSAM depicting Minor Victim 4 by "baiting" Minor Victim 4.

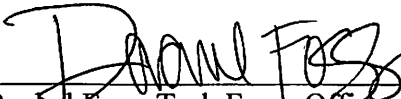
VI. CONCLUSION

71. Based on the facts set forth above, I respectfully submit that there is probable cause to believe that between on or about August 20, 2022, and on or about October 25, 2023, in

the Eastern District of Virginia and elsewhere, SHANNON ROBBINS violated 18 U.S.C. § 2252(a)(2), receipt and/or distribution of child pornography; 18 U.S.C. § 2252(a)(3), sales of child pornography; 18 U.S.C. § 2252(a)(4)(B), possession of child pornography; 18 U.S.C. § 2422(b), coercion and enticement of a minor; and/or 18 U.S.C. § 1470, transfer of obscene material to a minor.

72. Accordingly, I request that a complaint and arrest warrant be issued charging SHANNON ROBBINS with such offenses.

FURTHER AFFIANT SAYETH NAUGHT.



Rachel Foss, Task Force Officer
Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me on February 1, 2024.



UNITED STATES MAGISTRATE JUDGE